UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/659,129	09/10/2003	David G. Therrien	25452-013	3559

30623 7590 02/17/2009

MINTZ, LEVIN, COHN, FERRIS, GLOVSKY AND POPEO, P.C
ONE FINANCIAL CENTER
BOSTON, MA 02111

EXAMINER	
ADAMS, CHARLES D	

ART UNIT	PAPER NUMBER
2164	

MAIL DATE	DELIVERY MODE
02/17/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/659,129	THERRIEN ET AL.	
	Examiner	Art Unit	
	CHARLES D. ADAMS	2164	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *21 November 2008*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1,3-17 and 19-26* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1, 3-17, 19-26* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Remarks

1. In response to communications filed on 21 November 2008, claims 1, 7 and 17 are amended. Claims 1, 3-17, and 19-26 are pending in the application.

Claim Objections

2. Claim 17 is objected to because of the following informalities: newly added limitation states "wherein the protection policy is configured to be uniquely defined each share of date on the fileserver". Examiner believes this should read "each share of data", based on the context and amendments to claim 1. Appropriate correction is required.

Claim Rejections - 35 USC § 103

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

4. Claims 1, 6, 17, and 21-25 are rejected under 35 U.S.C. 103(a) as being unpatentable over Whiting et al. (US Patent 5,778,395), in view of Fujibayashi (US Pre-Grant Publication 2003/0131278) further in view of Zayas et al. (US Patent 6,560,615).

As to claim 1, Whiting et al. teaches a data protection system, comprising:

A fileserver configured to contain shares of data and to be connected with a repository (see 7:8-19 and 7:59-8:20),

Whiting et al. does not explicitly teach two or more repositories are configured to store a replica of a file, wherein a storage location and a number of replicas in each repository can be configured to change over time;

Fujibayashi teaches two or more repositories are configured to store a replica of a file, wherein a storage location and a number of replicas in each repository can be configured to change over time (see paragraphs [0019]-[0020]. A local storage is connected to a remote storage, to which it mirrors the data it stores. The remote storage snapshots contain copies of the local storage snapshots. The storage location is configured to change over time, as volumes are added and replace other volumes. The number of copies is configured to change over time, as more volumes are added from 1 to N);

Whiting et al. as modified teaches wherein:

The fileserver includes:

A filter driver operative to intercept input or output activity initiated by client file requests (see Whiting et al. 7:8-19 and 7:59-8:20)

Whiting et al. does not teach and further configured to capture a snapshot of a set of the shares of data at a particular point in time and to maintain a list of modified and/or created files since a last snapshot occurred.

Zayas et al. teaches and further configured to capture a snapshot of a set of the shares of data at a particular point in time and to maintain a list of modified and/or created files since a last snapshot occurred (see 5:31-40 and 7:16-46);

Whiting et al. as modified teaches a file system in communication with the filter driver and operative to store client files (see Zayas et al. 7:16-46 and Whiting et al. 7:8-19);

The filter driver is configured to capture the snapshot at a specified time interval based on a backup frequency defined in a protection policy stored in the fileserver, wherein the protection policy is configured to be uniquely defined for each share of data on the fileserver (see Whiting et al. 5:2-8 and 7:17-24. Each node has its own share of data, wherein each node can set its own protection policy).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to have modified Whiting et al. by the teachings of Fujibayashi, since Fujibayashi teaches "by locating data backups remotely, a customer can survive a disaster by restoring data using backed up data mirrored in a remote location that was unaffected by the disaster" (see paragraph [0002]).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to have modified Whiting et al. by the teaching of Zayas et al., since Zayas et al. teaches "insertion and removal of entries in the MFL are performed by the storage system. When the first of a file's data and metadata bits are turned on, the storage system adds the file to the MFL. In this way, a file is added only once to the MFL" (see 7:40-45).

As to claim 6, Whiting et al. as modified teaches: wherein the fileserver, based on the protection policy, is adapted to define repositories used for storage of files (see Whiting et al. 7:59-8:20), frequency of data backup (see Whiting et al. 5:2-8 and 33:49-51), how many replicas are maintained within each repository (see Whiting et al. 8:16-20), and how modifications to share data are maintained (see Whiting et al. 7:59-8:20).

As to claim 17, Whiting et al. teaches a data protection system comprising:

A fileserver configured to contain shares of data and to be connected with a repository (see 7:8-19 and 7:59-8:20)

Whiting et al. does not teach wherein two or more repositories are configured to store a replica of a file, wherein a storage location and a number of replicas in each repository can be configured to change over time;

Fujibayashi teaches wherein two or more repositories are configured to store a replica of a file, wherein a storage location and a number of replicas in each repository can be configured to change over time (see paragraphs [0019]-[0020]);

Whiting et al. as modified teaches:

Said fileserver includes:

Filter driver means for intercepting input or output activity initiated by client file requests (see 7:8-19 and 7:59-8:20)

Whiting et al. does not teach and for capturing a snapshot of a set of the shares of data at a particular point in time and for maintaining a list of modified and/or created files since a last snapshot occurred

Zayas et al. teaches and for capturing a snapshot of a set of the shares of data at a particular point in time and for maintaining a list of modified and/or created files since a last snapshot occurred (see 5:31-40 and 7:16-46)

Whiting et al. as modified teaches:

File system means in communication with the filter driver, the file system means for storing client files (see Zayas et al. 7:16-46 and Whiting et al. 7:8-19);

Wherein said filter driver means is configured to capture the snapshot at a specified time interval based on a backup frequency defined in a protection policy stored in the file server, wherein the protection policy is configured to be uniquely defined each share of date on the file server (see Whiting et al. 5:2-8 and 7:17-24. Each node has its own share of data, wherein each node can set its own protection policy),

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to have modified Whiting et al. by the teachings of Fujibayashi, since Fujibayashi teaches "by locating data backups remotely, a customer can survive a disaster by restoring data using backed up data mirrored in a remote location that was unaffected by the disaster" (see paragraph [0002]).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to have modified Whiting et al. by the teaching of Zayas et al., since Zayas et al. teaches "insertion and removal of entries in the MFL are

performed by the storage system. When the first of a file's data and metadata bits are turned on, the storage system adds the file to the MFL. In this way, a file is added only once to the MFL" (see 7:40-45).

As to claim 21, Whiting et al. as modified teaches wherein, based on the protection policy, the fileserver is further configured to determine whether to purge a file from a repository after the file has been deleted from a set of files (see Zayas et al. 7:11-15 and 8:5-14).

As to claim 22, Whiting et al. as modified teaches wherein, based on the protection policy, the fileserver is further configured to determine whether to keep a version history of a file in the set of files (see Whiting et al. 7:59-8:20 and 34:24-36).

As to claim 23, Whiting et al. as modified teaches wherein, based on the protection policy, the fileserver is further configured to determine a specified backup frequency for a repository (see Whiting et al. 5:2-8 and 33:49-51).

As to claim 24, Whiting et al. as modified teaches wherein, based on the protection policy, the fileserver is further configured to determine a specified type of compression for a file in the set of files (see Whiting et al. 8:21-40).

As to claim 25, Whiting et al. as modified teaches wherein, based on the protection policy, the fileserver is further configured to determine a specified caching level of a repository (see Whiting et al. 6:52-7:2).

5. Claims 3-5 and 20 are rejected under 35 U.S.C. 103(a) as being unpatentable over Whiting et al. (US Patent 5,778,395), in view of Fujibayashi (US Pre-Grant Publication 2003/0131278), in view of Zayas et al. (US Patent 6,560,615), and further in view of Belknap et al. (US Pre-Grant Publication 2003/0070001).

As to claim 3, Whiting et al. as modified teaches the system of claim 1.

Whiting et al. as modified does not teach a location cache configured to determine based on the protection policy which repository will be used to protect each share of data;

Belknap et al. teaches a location cache configured to determine based on the protection policy which repository will be used to protect each share of data (see paragraphs [0063]-[0064]).

Whiting et al. as modified teaches a location manager coupled to the location cache and operative to update the location cache when the fileserver protects a new share of data in a specific repository node (see Belknap et al. paragraph [0069]).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to have further modified Whiting et al. by the teaching of Belknap et al., since Belknap et al. teaches "to provide a common interface to media

servers which conceals the media server specific device commands from applications which interact with the media servers included within the system" (see paragraph [0006]).

As to claim 4, Whiting et al. as modified teaches:

A local repository in communication with the fileserver and adapted for receiving files from the fileserver (see Whiting et al. 7:59-8:20. Whiting et al. transfers items from a local database to a remote one):

A local repository node API adapted for communicating with the fileserver API (see Whiting et al. 7:59-8:20);

The local repository is further adapted to receive replicated files from the fileserver (see Whiting et al. 7:59-8:20); and

The local repository includes a protection policy component operative to determine whether new versions of existing files should be compressed and whether older versions of exiting files should be maintained (see Whiting et al. 7:59-8:20 and 34:24-36).

As to claim 5, Whiting et al. as modified teaches:

A remote repository in communication with the local repository and adapted for receiving files from the local repository (see Belknap et al. paragraph [0066] and Whiting et al. 6:52-7:2):

The remote repository is further adapted to receive replicated files from the local repository (see Belknap et al. paragraph [0066] and Whiting et al. 6:52-7:2);

The remote repository includes a protection policy component operative to determine whether new versions of existing files should be compressed and whether older versions of existing files should be maintained (see Whiting et al. 7:59-8:20 and 34:24-36).

As to claim 20, Whiting et al. teaches the system of claim 1.

Whiting et al. does not teach wherein, based in the protection policy, the fileserver is configured to determine the location of repositories

Belknap et al. teaches wherein, based in the protection policy, the fileserver is configured to determine the location of repositories (see paragraphs [0063]-[0064])

Whiting et al. as modified teaches and a number of replicas of the files to be stored in each repository (see Whiting et al. 8:16-20).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to have further modified Whiting et al. by the teaching of Belknap et al., since Belknap et al. teaches "to provide a common interface to media servers which conceals the media server specific device commands from applications which interact with the media servers included within the system" (see paragraph [0006]).

6. Claims 7-10, 13-16, and 26 are rejected under 35 U.S.C. 103(a) as being unpatentable over Parker et al. (US Patent 6,847,982) in view of Zayas et al. (US Patent 6,560,615), and further in view of Fujibayashi (US Pre-Grant Publication 2003/0131278).

As to claim 7, Parker et al. teaches a method for protecting data comprising:

Storing a version of a file within a set of files on a primary disk storage system (see 7:24-35);

Parker et al. does not teach capturing a snapshot of the set of files at a particular point in time

Zayas et al. teaches capturing a snapshot of the set of files at a particular point in time (see 7:16-46);

Parker et al. as modified teaches based on a backup frequency defined in a protection policy (see Parker et al. 7:32-34 and 9:6-11);

Maintaining a list of modified and/or created files since last captured snapshot (see Zayas et al. 5:31-40 and 7:16-46);

Examining the protection policy associated with the set of files to determine where and how to protect files associated with the set of files (see Parker et al. 7:34-35 and 9:23); and

Replicating the version of the file to two or more repositories specified by the protection policy, wherein the repositories includes at least one of a local repository and a remote repository (see Parker et al. 7:44-59 and 9:23)

Parker et al. does not teach:

wherein a storage location and a number of replicas of the version of the file can be configured to change over time.

Fujibayashi teaches wherein a storage location and a number of replicas of the version of the file can be configured to change over time (see paragraphs [0019]-[0020]).

Parker et al. as modified teaches wherein the protection policy is configured to be uniquely defined for each set of files (see Parker et al. 7:24-35. The protection policy is uniquely defined for the set of files to be captured. Also see 8:32-9:31, which lists out several different groups of files, and explains how a user can set options for each group).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to have modified Parker et al. by the teaching of Zayas et al., since Zayas et al. teaches "insertion and removal of entries in the MFL are performed by the storage system. When the first of a file's data and metadata bits are turned on, the storage system adds the file to the MFL. In this way, a file is added only once to the MFL" (see 7:40-45).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to have modified Parker et al. by the teachings of Fujibayashi, since Fujibayashi teaches "by locating data backups remotely, a customer can survive a disaster by restoring data using backed up data mirrored in a remote location that was unaffected by the disaster" (see paragraph [0002]).

As to claim 8, Parker et al. teachers wherein the file is configured to have at least one version (see Parker et al. 8:17-25 and Zayas et al. 6:65-7:15).

As to claim 9, Parker et al. teaches applying reverse delta compression to the versions of the file when a successive version of the file is stored in the repository (see Parker et al. 9:54-10:4).

As to claim 10, Parker et al. teaches wherein the step of applying reverse delta compression comprises:

Creating another version of the file, wherein the another version of the file is in a version of the file successive to the version of the file (see Parker et al. 9:54-10:4);

Replicating the another version of the file into the local repository and the remote repository (see Parker et al. 6:42-59 and 9:54-10:4);

Replacing the replicated version of the file in the local repository with a reverse delta compressed version representing a difference between the version of the file and the another version of the file and replicating; (see Parker et al. 9:54-10:4)

Transmitting the reverse delta compressed version to the remote repository (see Parker et al. 6:42-59. A reverse delta can be sent with the data with the shipping container as well as a forward delta); and

In the remote repository, replacing the version of the file with the reverse delta compressed version to store the another version and the reverse delta compressed

version (see Parker et al. 6:42-59 and Zayas et al. 7:25-32. A reverse delta can be sent with the data with the shipping container as well as a forward delta).

As to claim 13, Parker et al. teaches wherein examining a protection policy associated with the set of files to determine where and how to protect files associated with the set of files comprises:

Determining whether to keep a version history of a file in the set of files (see Zayas et al. 7:25-40 and Parker et al. 9:54-10:4).

As to claim 14, Parker et al. teaches wherein examining a protection policy associated with the set of files to determine where and how to protect files associated with the set of files comprises:

Determining a specified backup frequency for a repository (see Parker et al. 8:17-25 and 9:6-11).

As to claim 15, Parker et al. teaches wherein examining a protection policy associated with the set of files to determine where and how to protect files associated with the set of files comprises:

Determining a specified type of compression for a file in the set of files (see Parker et al. 6:42-59. A reverse delta can be chosen along with a forward delta to send to the library).

As to claim 16, Parker et al. teaches wherein examining a protection policy associated with the set of files to determine where and how to protect files associated with the set of files comprises:

Determining a specified caching level of a repository (see Parker et al. 9:12-14. A storing (caching) frequency level is determined and chosen).

As to claim 26, Parker et al. as modified teaches wherein the fileserver further includes:

backup means for backing up the modified files into repositories identified in the protection policy based on the backup frequency (see Parker et al. 9:6-11);

Storage means for storing a latest version of a file in a repository where a prior version of the file is stored (see Parker et al. 9:54-10:4);

Means for determining a difference between the latest version of the file and the prior version of the file (see Parker et al. 9:54-10:4);

Means for applying reverse delta compression of the difference (see Parker et al. 9:54-10:4); and

Means for replacing the prior version of the file with the reverse delta compressed difference between the latest version and the prior version of the file (see Parker et al. 9:54-10:4).

7. Claims 11-12 are rejected under 35 U.S.C. 103(a) as being unpatentable over Parker et al. (US Patent 6,847,982) in view of Zayas et al. (US Patent 6,560,615), in

view of Fujibayashi (US Pre-Grant Publication 2003/0131278) , and further in view of Santry et al. ("Deciding when to forget in the Elephant file system").

As to claim 11, Parker et al. teaches wherein examining a protection policy associated with the set of files to determine where and how to protect files associated with the set of files comprises:

Determining the location of repositories (see Parker et al. 10:36-55)

Parker et al. does not teach and a number of replicas of the files to be stored in each repository.

Santry et al. teaches a number of replicas of the files to be stored in each repository (see page 113, section 3.3. Only one version is kept).

Therefore, it would have been obvious to one of ordinary skill at the time the invention was made to have modified Parker et al. by the teaching of Santry et al., since Santry et al. teaches that "old versions of files are automatically retained and storage is managed by the file system. Users specify retention policies for individual files, groups of files, or directories. The goal of Elephant is to allow users to retain important old versions of all of their files. User actions such as delete and file write are thus easily revocable by rolling back a file system, a directory, or an individual file to an earlier point in time" (see page 111, last paragraph of section 1).

As to claim 12, Parker et al. teaches the method of claim 7.

Parker et al. does not teach wherein examining a protection policy associated with the set of files to determine where and how to protect files associated with the set of files comprises:

Determining whether to purge a file from a repository after the file has been deleted from a set of files.

Santry et al. teaches wherein examining a protection policy associated with the set of files to determine where and how to protect files associated with the set of files comprises:

Determining whether to purge a file from a repository after the file has been deleted from a set of files (see page 113, section 3.5 and 115, section 4.2.3 (it is determined whether a file should be deleted)).

Therefore, it would have been obvious to one of ordinary skill at the time the invention was made to have modified Parker et al. by the teaching of Santry et al., since Santry et al. teaches that "old versions of files are automatically retained and storage is managed by the file system. Users specify retention policies for individual files, groups of files, or directories. The goal of Elephant is to allow users to retain important old versions of all of their files. User actions such as delete and file write are thus easily revocable by rolling back a file system, a directory, or an individual file to an earlier point in time" (see page 111, last paragraph of section 1).

8. Claim 19 is rejected under 35 U.S.C. 103(a) as being unpatentable over Whiting et al. (US Patent 5,778,395), in view of Fujibayashi (US Pre-Grant Publication

2003/0131278) , in view of Zayas et al. (US Patent 6,560,615), and further in view of Burns et al. ("Efficient Distributed Backup with Delta Compression").

As to claim 19, Whiting et al teaches:

Backup said modified files into repositories identified in said protection policy based on said backup frequency (see Whiting et al. 5:2-8 and 33:49-51);

Store a latest version of a file in a repository where a prior version of said file is stored (see Whiting et al. 8:21-31);

Determine a difference between said latest version of said file and said prior version of said file (see Whiting et al. 8:21-31);

Whiting et al. does not teach to apply reverse delta compression to said difference;

Burns et al. teaches to apply reverse delta compression to said difference (see Burns et al. section 4.2);

Whiting et al. as modified teaches replace said prior version of said file with said reverse delta compressed difference between said latest version and said prior version of said file (see Burns et al. section 4.2).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to have further modified Whiting et al. by the teaching of Burns et al., since Burns et al. teaches that "by using delta compression algorithms, which minimally encode a version of a file using only the bytes that have changed, a backup system can compress the data sent to a server" (see Abstract).

Response to Arguments

9. Applicant's arguments with respect to the claims have been considered but are moot in view of the new ground(s) of rejection.

10. Applicant's arguments filed 1 December 2008 have been fully considered but they are not persuasive.

In regards to claim 1, Applicant argues that "however, Whiting fails to disclose that these created or modified files are replicas of a single file. In contrast, Whiting stores only a single copy of the file." In response to this argument, it is noted that Whiting et al. has the capability to store backup versions of a file as well as references to a file, if a backup version is already stored. However, Whiting et al. still teaches to store backup copies of a file, in the case that the file does not already exist. Thus, it would have been obvious to one of ordinary skill in the art the time the invention was made to have considered the situation where no copy previously exits, and only new copies are made.

Applicant continues, arguing "Further, Whiting's backup policy is the same for all sets of files, ie., the policy looks to a set of files to determine which files fall into one of the four categories specified above. This is different than having a protection policy uniquely defined for each share of data on the fileserver, as recited in the amended

claim 1." In response to this argument, it is noted that each local machine may have a unique backup schedule configured. This backup schedule is part of the "protection policy". It is also noted that each user machine receives its own share of data on the server (see 7:8-31).

Applicant argues that "Zayas further enumerates and orders all identified files in the MFL that were first modified before the selected epoch. This is different than having a filter driver configured to capture a snapshot of a set of the shares of data at a particular point in time, as recited in claim 1. Instead, Zayas only deals with specific identified files, i.e., only those that have been modified, rather than the entire set of shares of data, contrary to the recitation of the amended claim." In response to this argument, it is noted that the claims are directed towards "shares of data". No definition exists in the claims as to what "shares of data" entail. Examiner has interpreted "a set of shares of data" to mean "a set of files for backup".

Applicant argues that "Further, the present invention captures a snapshot of an entire file system at a specific point in time. Such snapshots are taken at specific periods of time, and lists of files are maintained since the last snapshot occurred. Such occurrence is different than enumeration and capture of files since their last archive." In response to this argument, it is noted that the claims are only directed towards capturing "a snapshot of a set of the shares of data at a particular point in time", rather than "an entire file system at a specific point in time".

Applicant argues that "one of ordinary skill in the art would not have combined the teachings of Whiting and Zayas in order to solve the deficiencies of Whiting. Since the references lack disclosure of" claim 1, "the combination of references fails to render claim 1 obvious". In response to this argument, it is noted that a newly cited reference, Fujibayashi has been added to the rejection. The combination of all three references would have made the currently claimed invention obvious to one of ordinary skill in the art.

In regards to Belknap et al., Applicant argues that "the present invention's location cache is configured to determine, based on the protection policy, which repository will be used to protect each share of data, as recited in the claims." In response to this argument, it is noted that the library server of Belknap et al. holds location information, which describe where to find shares of data, and store updates to them (see paragraphs [0063]-[0064]).

Applicant argues that Belknap et al. and Burns et al. fail to fill missing elements in either Whiting, Zayas, or their combination in regards to claim 1. In response to this argument, it is noted that

In regard to claim 7, Applicant argues that the inventions of Parker et al. and Zayas et al. are "different than replicating the version of the file to two or more

repositories specified by the protection policy, wherein the repositories include at least one of a local repository and a remote repository, wherein a storage location and a number of replicas of the version of the file can be configured to change over time". In response to this argument, it is noted that Fujibayashi et al. was added to the combination of the references to reject this limitation.

Applicant argues that "Parker discloses how files a the client are check-summed to determine whether their content changes over time and only those files that are new or have changed are sent to the Akashic Vault. However, Parker's policy is not uniquely defined for each set of files." In response to Applicant's argument, it is noted that no definition of what entails a set of files appears in the claim. It is also noted that Parker et al. teaches wherein the set of files that includes new and changed files is captured for backup. It is also noted that Parker et al. teaches wherein users can decide which files require capture, according to file type, file name, software program generated, or a number of other attributes (see 8:32-9:30).

Applicant argues that Santry et al. does not cure the deficiencies of Parker, Zayas, or their combination for claim 7. However, it is noted that Santry et al. is not relied upon to teach claim 7.

Conclusion

11. Any inquiry concerning this communication or earlier communications from the examiner should be directed to CHARLES D. ADAMS whose telephone number is (571)272-3938. The examiner can normally be reached on 8:30 AM - 5:00 PM, M - F.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Charles Rones can be reached on (571) 272-4085. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/C. D. A./
Examiner, Art Unit 2164

/Charles Rones/
Supervisory Patent Examiner, Art Unit 2164